UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/912,403	07/26/2001	William Michael Raike	P65847US1	4247

7590 08/05/2005

JACOBSON HOLMAN
PROFESIONAL LIMITED LIABILITY COMPANY
400 SEVENTH STREET, N.W.
WASHINGTON, DC 20004

EXAMINER	
NGUYEN, MINH DIEU T	
ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 08/05/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

4

## Office Action Summary	**Application No.** 09/912,403	**Applicant(s)** RAIKE, WILLIAM MICHAEL	
	Examiner Minh Dieu Nguyen	**Art Unit** 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 May 2005*.

2a)☒ This action is **FINAL**.   2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)□ Claim(s) _____ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the communication dated May 9, 2005 with the amendment to claims 1-8.

Response to Arguments

2. Applicant's arguments filed May 9, 2005 have been fully considered but they are not persuasive.

3. Applicant argues that there is no motivation to combine Levy et al. (6,212,633) with Wasilewski (5,420,866) and Bleichenbacher et al. (6,735,313). Levy was brought in to address the limitations of generating a random base key, encrypting the base key to create an open key and transmitting the open key to the recipient. Levy discloses a system to secure data communication between secured nodes incorporating data encryption and/or access control (col. 1, lines 18-20; col. 7, lines 39-42). Levy discloses memory mapped serial communications interface (i.e. IEEE1394), and further teaches IEEE 1394 specification defines both asynchronous and isochronous communications wherein streaming data such as audio or video data typically is transmitted via isochronous communications (col. 9, lines 2-9). Wasilewski and Bleichenbacher are both disclose transmitting of stream media, therefore it is proper to combine the references to address claimed limitations.

4. Applicant argues that none of the cited references discloses the feature of assigning a unique tag value to each packet in a data stream as in claims 1 and 6. The examiner disagrees, from the title and the abstract, Wasilewski discloses *packet-based* (for emphasis) multiplexed communications system. Wasilewski discloses each elementary stream to be transmitted is packetized to form a Packetized Elementary Stream (PES), each PES packet consists of a PES packet header and is assigned a unique "packet ID" (PID) (col. 1, lines 39-60). Wasilewski discloses a unique tag value is assigned to each packet (Fig. 3A, elements PID 10, PID 12 and PID 18; Fig. 3B, elements PID 27, PID 35; PID 92 etc.).

5. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

6. Applicant's arguments with respect to the rejection(s)of claim(s) 2 have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Wasilewski, Bleichenbacher, Levy and Hawthorne.

Claim Rejections - 35 USC § 112

7. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the

> art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

8. Claims 1 and 6 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. The specifications is not clear on defining a "unique tag value" although it states a "tag" uniquely identifies a packet (Specifications, page 3 lines 6-7).

Specification

9. The amendment filed May 9, 2005 is objected to under 35 U.S.C. 132(a) because it introduces new matter into the disclosure. 35 U.S.C. 132(a) states that no amendment shall introduce new matter into the disclosure of the invention. The added material which is not supported by the original disclosure is as follows: "assigning a *unique* tag value to each packet if no tag value already exists".

Applicant is required to cancel the new matter in the reply to this Office Action.

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claims 1, 3-6 and 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski (5,420,866) in view of Bleichenbacher et al. (6,735,313) and further in view of Levy et al (6,212,633).

a) As to claims 1 and 6, Wasilewski discloses methods for providing conditional access information to decoders in a packet-based multiplexed communications system comprising a transmitter (Fig. 2, element 198) encrypts payload sections of each transport packet stream of data (col. 9, lines 30-36) that assigned a unique packet ID (PID) (col. 8, lines 44-46) using unique encryption control words (col. 9, lines 26-30); transmitter adds the packet ID to the corresponding encrypted packet data; inserts the packet so processed into the packet stream and transmit the encrypted data packet stream to the recipient (Figs. 3A and 3B). Wasilewski also discloses at the recipient's station (Fig. 2, element 201), each received encrypted packet is decrypted by the decryption information respective to each packet ID (Fig. 6; col. 14, lines 13-20) and the decrypted packet data is outputted in a form suitable for playing the streamed media (Fig. 2, element 208).

Wasilewski does not disclose the encryption key used for encrypting packet data is created by computing a secure hash of a base key and the assigned tag value of the packet.

Bleichenbacher discloses a system for transmitting an encrypted program together with a program identifier which is used by a set top terminal, together with stored entitlement information, to derive the decryption key necessary to decrypt the program (col. 1, lines 9-15), the system comprising a program key used to encrypt each program (col. 3, lines 4-6), the program key is created by applying a hash function to the master key and program identifier (col. 3, lines 30-37). The master key which reads on the base key may be updated for security reason (col. 7, lines 21-23). Bleichenbacher also discloses the decryption process (Fig. 9).

Both Wasilewski and Bleichenbacher do not disclose encrypting the base key to create an open key and transmit the open key to the recipient.

Levy discloses a secure data communication incorporating data encryption and/or access control comprising the steps of generating randomly a session key, encrypting the session key (col. 13, line 64 to col. 14, line 3) and transmit the encrypted session key to target node (col. 14, lines 15-17).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of computing hash function of base key and packet ID as Bleichenbacher teaches in the system of Wasilewski and the use of encrypting the base key as Levy teaches in the system of Wasilewski and Bleichenbacher so as to enhance the security of transmitted information.

b) As to claim 3, Levy as mofied above discloses the base key is encrypted using a public key encryption algorithm in conjunction with the recipient's public key and wherein the open key is decrypted using the public key encryption algorithm in conjunction with the recipient's private key (col. 13, line 64 to col. 14, line 3).

c) As to claim 4, Wasilewski as modified above discloses the packet data is encrypted using a symmetric encryption algorithm in conjunction with the packet key and the encrypted data is decrypted at the recipient's station using the symmetric encryption algorithm in conjunction with the recreated packet key (col. 3, line 45 to col. 4, line 6).

d) As to claims 5 and 8, Bleichenbacher as modified above discloses the hash function used to create and reestablish the packet key is SHA-1 or MD5 (col. 5, lines 43-47).

12. Claims 2 and 7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski (5,420,866) in view of Bleichenbacher et al. (6,735,313) in view of Levy et al (6,212,633) and further in view of Hawthorne (5,768,381).

Wasilewski, Bleichenbacher and Levy do not disclose transmitting the open key to the recipient by adding it to the stream header and extracted from the stream header at the recipient's station for decryption.

Hawthorne discloses encryption and decryption of electronically transmitted messages (col. 1, lines 6-10) comprising transmitting encrypted session key (i.e. open key) as header to the recipient and at the recipient station the encrypted session key is extracted for decryption (col. 5, lines 50-67; Fig. 7).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of transmitting the open key to the recipient by adding it to the stream header and extracted from the stream header at the recipient's station for decryption in the system of Wasilewski, Bleichenbacher and Levy as Hawthorne teaches so as to strengthen secure communications between two entities.

Conclusion

13. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

14. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dieu Nguyen whose telephone number is 571-272-3873. The examiner can normally be reached on M-F 6:00-2:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

Minh Dieu Nguyen
Examiner
Art Unit 2137

mdn
7/27/05

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER